

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04M 1/00, G06K 19/07, G06F 15/02, G07B 15/02		A1	(11) International Publication Number: WO 96/34483 (43) International Publication Date: 31 October 1996 (31.10.96)
(21) International Application Number: PCT/EP96/01739 (22) International Filing Date: 26 April 1996 (26.04.96) (30) Priority Data: 1000254 28 April 1995 (28.04.95) NL 1002112 17 January 1996 (17.01.96) NL (71) Applicant: KONINKLIJKE PTT NEDERLAND N.V. (NL/NL); Stationsplein 7, NL-9726 AE Groningen (NL). (72) Inventors: PIETERSE, Rob; Verbenalaan 1, NL-2111 ZL Aerdenhout (NL). DE LANGE, Martin; Kinn; Kers engarde 188, NL-2272 NN Voorburg (NL). PORS, Mark; Albert; Okenhout 71, NL-2719 KV Zoetermeer (NL). VAN TILBURG, Johan; Jonkerbos 141, NL-2715 SR Zoetermeer (NL). VAN POMEREN, Frank; Pieter; J. Camperlaan 37, NL-2624 NZ Delft (NL).			(81) Designated States: AU, BG, BR, BY, CA, CN, CZ, EE, HU, JP, KR, LT, LV, MX, NO, NZ, PL, RU, SG, UA, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>
(54) Title: A DEVICE FOR TRANSPARENT INTERACTION BETWEEN AN IC CARD AND A REMOTE TERMINAL			
<p>The diagram illustrates the system architecture. A telephone set (13) is connected to a device (1) through a cable (11). The device (1) is connected to a communication network (41) via a cable (43). The communication network (41) is connected to a remote terminal (42) via a cable (44). The remote terminal (42) is connected to a service provider (SM) via a cable (44).</p>			
(57) Abstract			
<p>The invention provides a device (1) for providing a transparent exchange of commands and data between an IC card (11) and a remote terminal (42) via a communication network (41). The device (1) acoustically couples the IC card (11) with a telephone set (43). In order to speed up the exchange of data and commands, the device (1) preferably utilizes high level commands which represent several low level card commands. However, low level commands may also be transparently passed as a special high level command. The device (1) is inexpensive but allows an efficient use of IC cards for e.g. payment and identification purposes.</p>			

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Ghana	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CN	Switzerland	LJ	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

A device for transparent interaction between an IC card and a remote terminal.

BACKGROUND OF THE INVENTION

The invention relates to a device for interaction between an IC card and a remote terminal. More in particular, the invention relates to a device which enables a direct interaction between an IC card and a remote terminal, using a communication system.

Nowadays, there is an increasing demand for remote services. Thus through television various products and services are offered which consumers can order at home. Such services include "video on demand" (VOD), tele-shopping and tele-entertainment. Consumers want a prompt delivery of products ordered or a prompt access to entertainment services, such as video on demand. In order to prevent abuse of this kind of services, either an immediate payment should be made, or the identity of the user should be verified, before performing the service.

IC cards or smart cards are widely used today for effecting payments in e.g. public telephones (pay phones). An IC card contains an integrated circuit (IC) with a memory and, in more advanced cards, also a microprocessor. Such cards allow to make payments by deducting an amount to be paid from a balance on the card. In advanced cards such payments are secured by protocols involving the cryptographic processing of certain data and the use of associated keys. In this respect, reference is made to e.g. EP 0 637 004 and US 5 247 578.

Advanced IC cards also allow the identity of the card to be established, e.g. by transmitting a (cryptographically processed) card identity number. If access to the card is protected by means of e.g. a secret personal identification

number (PIN), the card may be employed for user verification, i.e. for securely establishing the identity of the user. Such a user verification is not only necessary when a prompt service is desired, but also when payment transactions without an instantaneous delivery of a service or product are carried out in a remote manner (e.g. tele-banking).

Presently, payment systems exist, such as the credit card systems, with which payment information is sent to a payment organisation via a telephone set. For this kind of transactions, the telephone set concerned is especially adapted with a card reader and, optionally, with a keyboard. Such devices have the disadvantage that they are relatively expensive. It is not to be expected that large numbers of consumers will within the foreseeable future buy such a device.

Furthermore, it is known in practice to communicate, via a standard telephone set, a credit card number in an oral manner. This has the disadvantage that third parties (e.g. by intruding the telephone connection) can easily abuse the number.

Several devices for communicating with an IC card are known from the Prior Art. US 5 189 287, for example, discloses a system for transmitting data. The system comprises portable units, each provided with a card slot for receiving a dual chip memory card in which data are stored, and optical and acoustical transceivers for exchanging information with special optical terminals and with remote systems via a telephone network, respectively. The units comprise processing means, such as a microprocessor, for processing data which may be manually entered using a keyboard.

WO 95/04328 also discloses a device for communicating with an IC card. This Prior Art device comprises a microcomputer and an associated operating system, arranged for running application programs. The device is

arranged for the processing and storage of financial data, the processing comprising the cryptographic processing of the data.

WO 91/07042 discloses a portable automated teller machine. The device, which comprises a microprocessor, operates without the need for a
5 direct connection to a telephone line and is thus basically a stand-alone unit.

EP 0 451 288 discloses a portable data collection and transmission device for use with an IC card. The device, which comprises an acoustic coupler to communicate via a telephone line, further comprises a memory for storing data. Stored data can thus be transmitted.

10 WO 94/28498 discloses a device for communicating with an IC card. The device does not have acoustic means for communicating with a telephone set but needs a separate connection to a subscriber line.

These Prior Art devices are basically stand alone units, provided with a microprocessor or the like for processing data independently from a remote
15 terminal or system.

SUMMARY OF THE INVENTION

An object of the invention is to eliminate above-mentioned and other disadvantages of the prior art and to provide a device which enables carrying
20 out a protected information exchange in a simple and inexpensive manner, especially for the purpose of remote user identification.

Another object of the invention is to provide a device for user verification over a communication system, particularly over a non-protected telecommunication system such as the public telephony system.

25 A further object of the invention is to provide a device for carrying out, in a remote manner via a telephone connection, a secure user verification for the purpose of electronic services, such as electronic payment transactions.

A still object of the invention is to provide a simple and inexpensive system for electronic payment transactions on the basis of communication means which already exist or are at least are not specifically equipped for user verification.

- 5 A yet further object of the invention is to provide a device for use in combination with a telephone set and an IC card, which device enables a more efficient exchange of secure messages.

To this end, the invention provides a device for exchanging data between an IC card and a remote terminal via a communication apparatus, the
10 device comprising means for connecting with the IC card; means for acoustically transmitting information to the communication apparatus; means for acoustically receiving information from the communication apparatus; and control means, which means are mutually coupled for the purpose of exchanging information between the communication apparatus and the IC
15 card, which device according to the invention is characterised in that it is arranged for the transparent transfer of data.

The present invention is based on the insight that for a secure communication between an IC card and a remote system, use can effectively be made of the features of present day cards (smart cards). In effect, by
20 utilizing the intelligence of the card, the intelligence of the device can substantially be dispensed with. By providing a transparent transfer of data, the device can be kept simple while the secure exchange of data between the IC card and the remote terminal is substantially left intact. By providing a transparent transfer device, a secure and reliable end-to-end communication
25 between the IC card and the remote terminal is made possible.

A preferred embodiment of the invention is also based on the further insight that the acoustic path between the transfer device and the telephone

set is limited in speed, while a secure use of IC cards involves the time-consuming exchange of a plurality of commands and other data between the IC card and the remote system. To solve this further problem, the device of the present invention is preferably arranged for communicating with the remote terminal on a first level and with the IC card on a second level, each level involving a different data rate. In this way, the transparent exchange of data can be adapted to the particular transmission path.

Preferably, in the device according to the invention a command of the first level comprises a single command of the second level. By retaining a one-to-one relationship between commands of the two levels, it is possible to pass a second level command as a first level command from the remote terminal to the device of the invention. Advantageously, however, a command of the first level represents one or more commands of the second level. In this way, the number of second level commands which need to be exchanged between the device and the remote terminal can be drastically reduced.

Furthermore, the invention provides a system for electronic payment transactions, comprising a telecommunication network, a service provider which is coupled to the network, which service provider is arranged for carrying out electronic payment orders, a communication apparatus which is also coupled to the network, an electronic IC card which is arranged for secured transactions, and a device for transparently passing data between the IC card and the communication device.

The invention is thus based on the understanding that only a coupling between an intelligent card (smart card) and a communication apparatus has to be set up in order to enable a safe remote card and/or user verification for services.

EXEMPLARY EMBODIMENTS

Hereinafter, the invention will be elucidated more in detail with reference to the Figures.

- 5 Fig. 1 shows a side and top view of a first embodiment of a device in accordance with the invention;
- Fig. 2 shows in a perspective view a second embodiment of a device in accordance with the invention;
- Fig. 3 shows the embodiment of Fig. 2 in a side view;
- Fig. 4 shows diagrammatically the internal structure of a device
10 in accordance with the invention;
- Fig. 5 shows diagrammatically an alternative internal structure of a device in accordance with the invention;
- Fig. 6 shows diagrammatically the exchange of messages between the constituent parts of a remote payment system in
15 accordance with the invention;
- Fig. 7 shows diagrammatically an embodiment of a payment system in accordance with the invention.

A preferred embodiment of a device in accordance with the invention is represented, by way of example, in Fig. 1. The devices 1 shown in Fig. 1
20 comprise a housing 2, a microphone 3, a loudspeaker 4, a display 5, a control button 7, and keys 9. In the housing 2, a slot 8 has been recessed for inserting an IC card 11. The side view of the device 1 shows a connector 12 for (serial) data exchange with e.g. a computer.

25 The microphone 3 and the loudspeaker 4 constitute acoustic transducers for converting electrical signals into acoustic signals (for instance DTMF tones) in order to establish an information exchange between IC card 11 and a communication apparatus, such as a telephone set. Although they are

shown as separate units in Fig. 1, the microphone 3 and the loudspeaker 4 may be combined into a single unit.

The device 1 can be activated by the control button 7. However, the device may also be activated by an internal switch which acts upon the presence of a card 11, in which case the control button 7 may be omitted. The display 5, which preferably is constituted by an LCD display screen, serves as an indicator of the status of the device in order to facilitate its use. Alternatively, LEDs (not shown) or a tone and/or voice generator can be used for this purpose. In latter case, the loudspeaker 4 can advantageously be used for the purpose of indicating status. The keys 9 serve to enter data, such as a personal identification code (PIN) of the user of the IC card 11.

The housing 2 preferably has a such a form that, while using the device 1, it can be held easily in one hand. This criterion is met with the shape shown in Fig. 1, but could also be met with e.g. a round or oval shape.

The alternative embodiment of the device 1, shown in Figs. 2 and 3, in accordance with the invention comprises a housing 2, a microphone 3, a loudspeaker 4, a first LED 5, a second LED 6, and a control button 7. In the embodiment shown, the housing 2 is composed of two parts 2a and 2b, which are interconnected by means of a hinge 10. In the housing 2 (part 2a) a slot 8 is recessed for inserting an IC card 11. Furthermore, the device 1 comprises keys 9 for entering, inter alia, numerical data. The housing, which is composed of the two parts 2a and 2b, is preferably implemented in such manner that it can be folded and unfolded. In the folded state, inter alia, keys 9 and the microphone 3 are protected; in the unfolded state, the distance between microphone 3 and loudspeaker 4 is approximately as large as the distance between loudspeaker 14 and microphone 15 of the receiver 13 of a telephone set. Possibly, the hinge 10 can be realised in such manner that when

unfolding the housing, the device is automatically activated so that the control button 7 can be omitted.

The receiver or handset 13, shown in Figs. 2 and 3, is provided with a loudspeaker 14 and a microphone 15. A cord 16 connects the receiver 13 to a
5 communication apparatus, such as a telephone set (not shown).

The mode of operation and the use of device 1 will be further explained later with reference to Figs 4-7.

In Fig. 3, device 1 and receiver 13 of Fig. 2 are shown in a side view. As shown in Fig. 3, when the device 1 is used, the loudspeaker 4 is situated in the vicinity of the microphone 15 of the receiver 13. Moreover, the
10 microphone 3 of the device 1 is then situated in the vicinity of the loudspeaker 14 of the receiver 13. For the protection of the microphone 3, it has been arranged in such manner that it is protected by the part 2b in folded state of the housing 2. This positioning at the "interior" in practice does not
15 prove to pose a problem. Possibly, the microphone 3 can be arranged at the other side of part 2b. It is noted, that for the sake of clarity, the microphone has been shown spherical in Fig. 3; however, in practice a flat microphone can also be used.

The device in accordance with the invention can be realised as a device
20 which can be held in one hand, as is shown in the Figs. 1, 2, and 3; however, it can also be realised as a "table-top version" on which a receiver of a telephone set can be placed. Furthermore, the device in accordance with the invention may be implemented as being integrated in or/and coupled to a telephone set or other communication device, such as a facsimile apparatus.

25 The internal composition of the device (1 in the Figs. 1, 2, and 3) in accordance with the invention and diagrammatically shown by way of example in Fig. 4 comprises a control unit 20, a coupling circuit 21, a card connector

22, a loudspeaker 23, a microphone 24, a signalling unit (optional) 25, a keyboard (optional) 26, and a power supply 27. For the sake of clarity, the housing 2 is not shown in Fig. 4. The loudspeaker 23 and the microphone 24 may correspond to the microphone 3 and the loudspeaker 4 respectively of the Figs. 1, 2, and 3. The optional keyboard 26 may be constituted by the keys 9 in the Figs. 1, 2 and 3.

In the housing (2 in the Figs. 1, 2, and 3) of the device, a space has been recessed in which an IC card can be inserted via a slot (8 in the Figs. 1 and 2). In this space, the card connector 22 has been arranged for providing a mechanical and electric contact with the IC card. Such a connector can be implemented in accordance with Standard ISO 7816. In case so-called contactless cards are used, the connector can advantageously be replaced by suitable (electromagnetic) means for exchanging information with the card, such as a transceiver provided with suitable antenna means.

The coupling circuit 21, which provides the coupling between, on the one hand, connector 22 and, on the other hand, loudspeaker 23 and microphone 24, for instance comprises a DTMF transducer 28, a multiplexer or fork circuit 29 and an (optional) rate adaptor 30. Under the influence of control unit 20, information is exchanged between the connector 22 (and the IC card connected thereto) and an (acoustic) transducer 31, which is constituted by the microphone 24 and the loudspeaker 23. The acoustic transducer 31 transforms electrical signals into acoustic signals and vice versa. Possibly, the transducer 31 can be implemented in such manner that it conducts a transduction between electric and optical signals, in which case the loudspeaker 23 would be replaced by e.g. an infrared transmitter and the microphone 24 e.g. by an infrared receiver. Another possibility would be to replace the transducer 31 by a line interface which provides an (electric)

coupling between the device and a communication network.

The signalling unit 25 attends to the signalling to the user, e.g. indicating the status of the device by means of, for example, the LEDs 5 and 6 shown in Fig. 2. Advantageously, the signalling unit 25 can be provided with
5 a voice generator for producing spoken instructions for the user.

The power supply 27 is preferably formed by a battery, but can also comprise a coupling to the power supply of a telephone set. The device in accordance with the invention can be provided with a keyboard 26 (keys 9 in Fig. 2) for entering a code. Said code may comprise a Personal Identification
10 Number (PIN) or a telephone number or access code, respectively, for example of an institution for effecting payments. Telephone numbers and/or access numbers may also be entered via the keyboard and be stored in the device and/or the IC card. When ISDN is used (for example via the so-called SBus), the keyboard 26 may be used for entering access numbers. Possibly,
15 the keyboard 26 can also be suited for entering non-numerical data (alpha numeric keyboard).

The device in accordance with the invention can be used in the following way. The user pushes the control button (7 in the Figs. 1, 2, and 3), upon which the device is activated. The first LED (5 in Fig. 2) blinks, in
20 order to indicate that the device is active. At all times the device, and consequently the IC card, can be blocked or de-activated by depressing the control button again.

The user then places the device 1 near the receiver (13 in the Figs. 2, 3, and 7) of the communication apparatus (e.g. a telephone set) and enters his
25 identification code (for example a PIN) on the keyboard 26. If the device 1 is not provided with a keyboard, the code may be entered on the communication apparatus. A period of time can also be entered, for example a maximum time

limit of the verification session or of using the service concerned. With the identification code, the IC card is activated. It should be understood that the identification code itself need not be transmitted to the communication apparatus, only to the IC card. This further enhances the security of the device.

Subsequently, the user dials the number (for example the telephone number) of the service or organisation desired, by entering this number on the keyboard of device 1 or of the telephone set (43 in the Figs. 5 and 6). If the number is stored in the device or in the payment means, this number can be issued automatically. Then, the verification session between the service provider (service organisation or institution) and the IC card is started.

In the first part of the session, the user places the microphone (3 in the Figs. 1, 2, and 3) of the device 1 near the loudspeaker (14 in Figs. 2 and 3) of the telephone handset 13 in order to receive information. If this has proceeded well, the first LED (5 in Fig. 2) starts to light up permanently and the second LED (6 in Fig. 2) starts blinking in order to indicate to the user that the second part of the session can commence. To this end the user places the loudspeaker (4 in the Figs. 1, 2, and 3) in the vicinity of the microphone (15 in the Figs. 2 and 3) of the receiver (13 in the Figs. 2 and 3). If transmitting information by the device 1 proved to be successful, the second LED (6 in Fig. 2) will start to light up permanently. This completes the transaction (e.g. user verification or payment). Preferably, the service provider or institution for effecting payments will give a return signal to the user via the device 1. When the session is completed, both LEDs will extinguish.

The above scenario is only given by way of example; it will be understood that many other scenarios are possible.

The device in accordance with the invention can be provided with

means (known per se) for voice recognition. First, it is then possible to make the device 1 voice-controlled, so that pushing the control button and keys can be omitted. This is especially, but not exclusively, advantageous for ill-sighted persons or disabled persons. Second, it is possible to offer an additional user verification by means of voice verification, that is to say, to identify the speaker unambiguously on the basis of his voice. Possibly, entering a PIN code can then be omitted.

The information which is exchanged via the device 1 between the telephone set and the IC card, can comprise at least three kinds of information. First, identification or verification information for verifying the identity of the user. After all, before a payment can be charged to an account, the user identity must be established. The information exchanged may further comprise payment information. That is, in the case of debiting a card, information relating to the balance remaining on the card and the value which must possibly be written off the card. Furthermore, dialling information can be exchanged, or can at least be emitted to the telephone set by the device. Possibly, the telephone set can emit dialling information to the device for the purpose of later usage (requesting an access number of a payment organisation). Said dialling information can for example be stored in the IC card.

As appears from the above, device 1 forms an interface between the telephone set and the IC card, transferring information in two directions. The facilities of the IC card (processor and memory with verification algorithm) may be used for performing a user verification and/or a card verification (which verification is preferably protected in a cryptographic manner). Since the built-in facilities of the IC card are utilized and the device basically only passes commands and/or data in a transparent manner, the device 1 can be

very simple and therefore inexpensive. Furthermore, the device in accordance with the invention is interchangeable, that is to say, the device can be used by different persons which each have their own IC card.

The device 1 may be composed of commercially available components.

5 The control unit 20 can be formed by a microprocessor and a memory. An additional memory (not shown in Fig. 4) may be provided for e.g. storing access codes and/or PIN codes. Preferably, the various electronic components, such as the control unit 20, the coupling circuit 21 and the signalling unit 25 are accommodated in a single application-specific integrated circuit (ASIC).

10 Fig. 5 shows an alternative internal arrangement of the device according to the invention. In the arrangement shown, the control unit 20 is constituted by a micro-controller, i.e. a microprocessor with a built-in memory and possibly additional circuits. As the micro-controller 20 preferably comprises input and output ports (UART), the multiplexer 29 and the rate
15 adaptor 30 may be omitted. The DTMF transducer 28 has been replaced by a modem. A display 32 is connected to the micro-controller 20. An erasable programmable memory (EPROM) 33, which may be constituted by an EEPROM or a so-called flash EPROM, serves to store suitable software of the micro-controller 20. Preferably, the device allows the software in the memory
20 33 to be upgraded, e.g. by loading new software from an IC card inserted into the device.

An (optional) serial connector 34 serves to provide a direct electrical connection, e.g. according to the RS232 protocol, with external devices, such as computers. This allows the device to be used for computer network
25 applications, e.g. performing payments via the Internet. The (optional) signalling unit 25 may be constituted by one or more LEDs.

The control unit or micro-controller 20 serves primarily to pass card

data (i.e. commands and card data proper) between the card connector 22 and the modem 28. Although the micro-controller 20 (and thus the transfer device 1) is basically transparent in that card data (i.e. card commands and card data proper) are merely passed through, the micro-controller preferably performs
5 an adaption of the card data in order to increase the speed at which card data are exchanged. This will further be explained with reference to Fig. 6.

In Fig. 6, the exchange of card data (commands and data sent to the IC card and their responses) between an IC card on the one hand and a secure module of a transaction unit on the other hand is schematically represented.
10 The IC card may correspond with the card 11 of Figs. 1, 2, 3 and 7, the transfer device may correspond with the device 1 of Figs. 1, 2 and 3, the transaction unit may be a computer or similar device incorporated in the service provider unit 42 of Fig. 7, and the secure module may correspond with the Secure Module (SM) 44 in Fig. 7.

15 In accordance with a further aspect of the present invention, a distinction is made between two levels of card commands exchange. Between the IC card and the transfer device, a low level exchange takes place: the actual card commands and card data are sent to and received from the card. As this exchange is performed using electrical signals within the transfer
20 device 1, the exchange can have a high data rate. Between the transfer device and the transaction unit, however, an acoustic path is present (between the device 1 and the receiver 13). This section of the connection between IC card and secure module usually has a limited transmission speed. For this reason, in this section a high level exchange takes place in which several low level
25 commands are grouped together and are replaced with a single high level command. In this way, the transmission time required for a transaction can be significantly reduced.

As is shown in Fig. 6, the transaction unit may issue a high level command (indicated by H). In response to the receipt of this single high level command, the transfer device exchanges several low level commands (indicated by L) with the IC card. The result of this exchange is sent by the transfer device to the transaction unit as a single high level command (H). Subsequently, this high level command results in the exchange of several low level commands (L) between the transaction unit and the secure module. Each high level command (H) thus represents a routine comprising a plurality (e.g. five of ten) low level commands (L). Preferably, the high level commands are optimized for efficiency by e.g. having each commonly used routine represented by a single high level command.

Preferably, the transfer device supports two different modes of data exchange. In a first mode (indicated by Mode I in Fig.6) the transfer device operates as described above: a high level command represents several low level commands. In a second mode (indicated by Mode II in Fig.6) a single low level command (L) is sent as a high level command (H') to the transfer device, which passes the command as a low level command to the IC card. The resulting low level command (L) produced by the card is again sent by the transfer device to the transaction unit as a high level command (H'), which subsequently converts the command back into a low level command (L). It will be understood that the high level commands H' merely convey low level commands (L). That is, the high level commands H' may e.g. consist of a low level command plus an appropriate header. In this way, low level commands may be transparently passed to the IC card while using the structure and/or data protocol of the high level commands. This transparent passing has the advantage that low level commands may be used for which no high level command is available, i.e. which cannot be grouped in an existing

high level command. This is especially advantageous as the introduction of an IC card with one or more new commands does not necessitate the upgrade of the software of the transaction device.

Preferably, the transfer device, as well as the transaction unit, is
5 capable of shifting back and forth between Mode I and Mode II, so that high level commands (H) representing a number of low level commands may be interspersed with high level commands (H') merely conveying a single low level command.

The (payment) system 40, shown in Fig. 7, comprises a tele-
10 communication system 41, which can comprise a telephone network. A service providing organisation 42 is coupled to the telecommunication system 41. This organisation 42 for example is a institution for effecting payments (such as a bank) which is arranged for paying in an electronic manner and therefore for executing verification procedures. The service provider 42 may not only be a
15 payment organisation but also a service-providing organisation in general (video centre; pizza courier). The transaction unit of the service provider 42 comprises a secure module (SM) 44 in which payment data and cryptographic keys are securely stored. It will be understood that for the sake of clarity only a single service provider 42 is shown in Fig. 7 but that in practice a plurality
20 of service providers 42 may be connected to the network 41.

A telephone set 43, which is also coupled to the telecommunication system 41, comprises a receiver 13. Via a device 1 in accordance with the invention (which corresponds with the device 1 of Fig. 1), an IC card 11 can, when being brought into contact with device 1 of Fig. 1, exchange
25 information with telephone set 43 and thus with the organisation 42. By means of exchanging verification information the identity and access authorization of the user of the IC card (verification card) 11 can be checked. Also, the

authenticity of the card 11 may be verified in this manner.

It will be understood that whenever "telephone sets" are mentioned in this text, these must not only include fixed, but also mobile telephone and/or facsimile sets (in general: communication apparatus). Such a communication apparatus can also be formed by a computer (such as a PC) with a microphone. Furthermore, the term "electronic payment transactions" will primarily, but not exclusively, mean remote paying, in other words paying via a (tele) communication device. Said paying remotely can for example be conducted by a customer at home, or by a customer in his office. The invention is especially suitable in combination with television broadcasts with the possibility of immediately ordering and paying advertised products.

The IC card mentioned in this text in general will be an electronic means for effecting payments, having an electronic circuit, arranged on a plastic substrate such as a so-called smart card or chip card. It will, however, be understood that the IC card need not have a cardlike shape. It is only essential, that the IC card can be used for performing a verification procedure, viz. the unambiguous determination of the authenticity and possibly also the identity of the card. Thus the access authorization of the card and/of the user can be checked ("authentication"). Therefore, the term "means for effecting payment" must not only include a IC card, but for example also an electronic module having an electronic circuit suitable for verification purposes. The integrated circuit needed for verification (for example a so-called ASIC) can possibly also be arranged in the device in accordance with the invention, without a card or such substrate. This can for example be realised by making an opening in the housing (compare the slot 8 in Fig. 1) in which an integrated circuit can be inserted in an un-detachable manner. This still offers the advantage that the device itself can be realised in

a very simple and therefore inexpensive manner.

A financial transaction, executed with the assistance of the device in accordance with the invention possibly not only comprises a payment transaction but also a loading (revaluing) transaction, in which the balance of the IC card is increased instead of decreased. Furthermore, transactions are possible in which the device in accordance with the invention is only used for verification purposes, and the balance on the card is not decreased. It has to be noted, in this context, that the mentioned IC card or "payment card" actually need not comprise a balance of payments but can also be used only for verification purposes (verification card).

Apart from financial transactions, the device in accordance with the invention can also be used in other transactions in which an information exchange takes place between an IC card and a telecommunication system. Thus with the device in accordance with the invention, an IC card, especially an identification or verification card, can be used with telephonic referenda and polls.

It will be understood by those skilled in the art that the invention is not limited to the embodiments represented and that various modifications and additions are possible without departing from the scope of the invention.

CLAIMS

1. Device (1) for exchanging data between an IC card (11) and a remote terminal (42) via a communication apparatus (43), the device comprising:
 - means (22) for connecting with the IC card (11);
 - 5 - means (23) for acoustically transmitting information to the communication apparatus (43);
 - means (24) for acoustically receiving information from the communication apparatus (43); and
 - control means (20),
- 10 which means (20, 22, 23, 24) are mutually coupled for the purpose of exchanging information between the communication apparatus (43) and the IC card (11), characterised in that the device is arranged for the transparent transfer of data.
2. Device according to claim 1, in which the device (1) is arranged for
- 15 communicating with the remote terminal (42) on a first level and with the IC card (11) on a second level, each level involving a different data rate.
3. Device according to claim 2, in which a command of the first level (H*) comprises a single command of the second level (L).
4. Device according to claim 2 or 3, in which a command of the first level
- 20 (H) represents one or more commands of the second level (L).
5. Device according to any of the preceding claims, comprising a reprogrammable memory (33).
6. Device according to any of the preceding claims, provided with a keyboard (9; 26) for entering data such as identification codes.
- 25 7. Device according to any of the preceding claims, provided with means for voice recognition.
8. Device according to any of the preceding claims, provided with a

housing (2) for hand-held use.

9. Financial transaction, carried out with a device (1) according to any of the preceding claims.

10. System (40) for electronic payment transactions, comprising a tele-communication network (41), a service provider (42) which is coupled to the network (41), which service provider (42) is arranged for carrying out electronic payment orders, a communication apparatus (43) which is also coupled to the network (41), an electronic IC card (11) which is arranged for secured transactions, characterized by a device (1) for transparently passing data between the IC card (11) and the communication device (43).

1/6

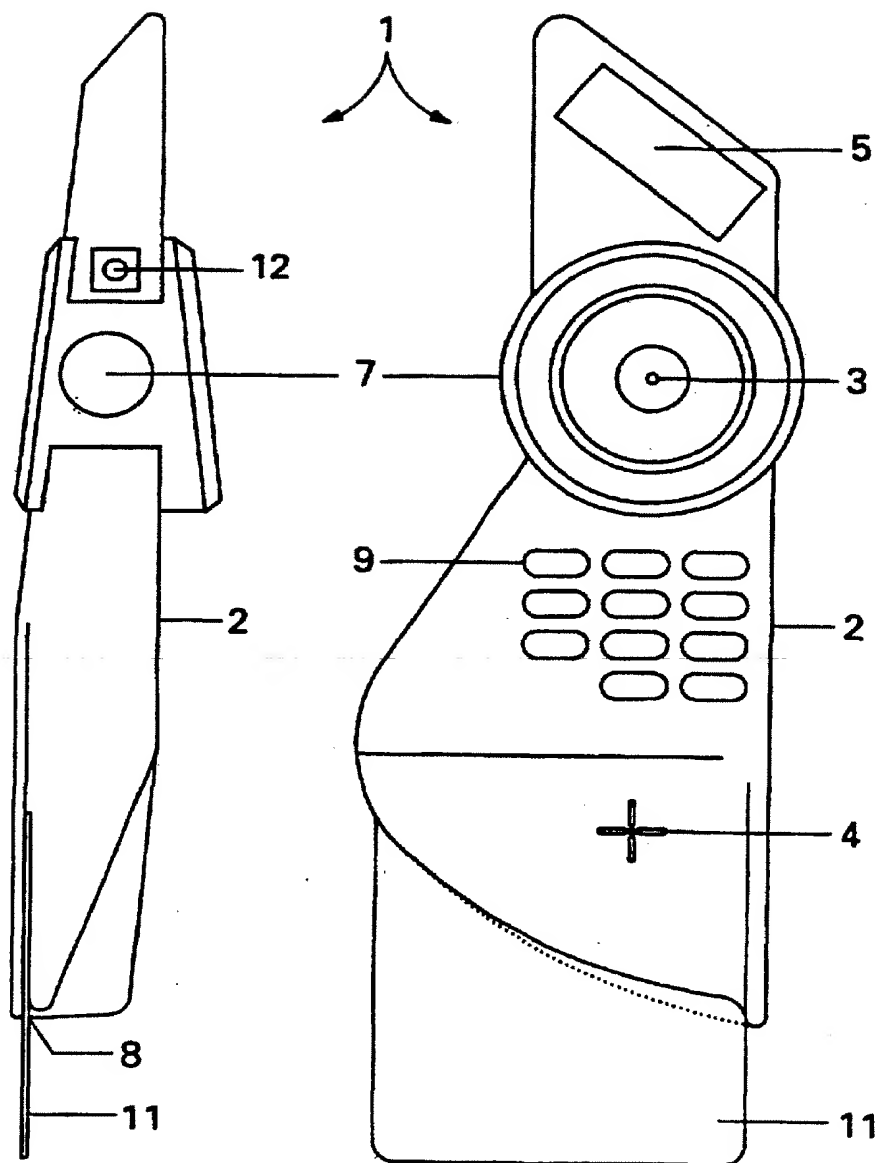


Fig. 1

2/6

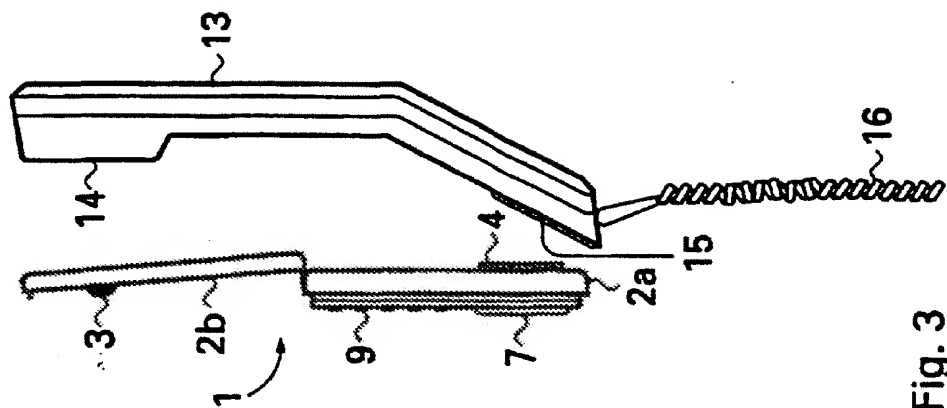


Fig. 3

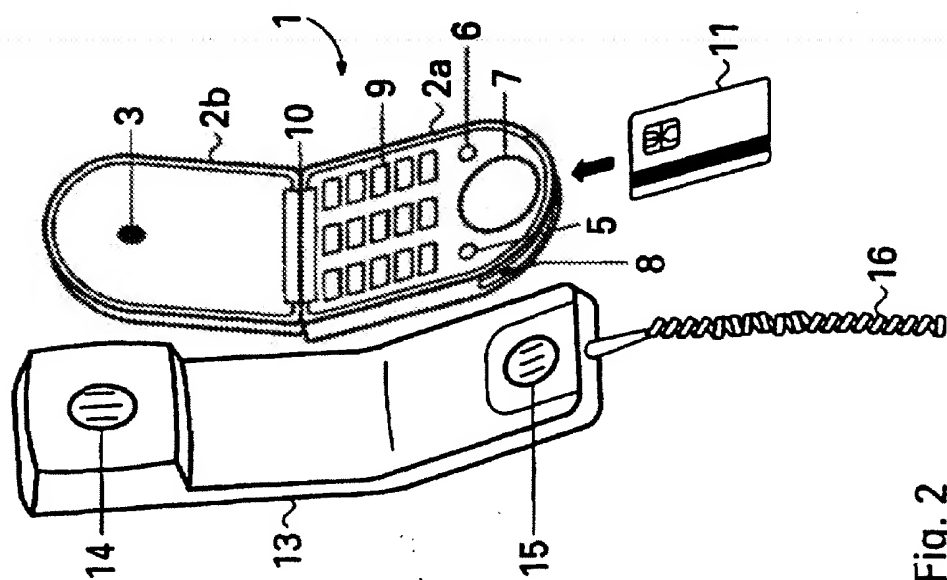


Fig. 2

3/6

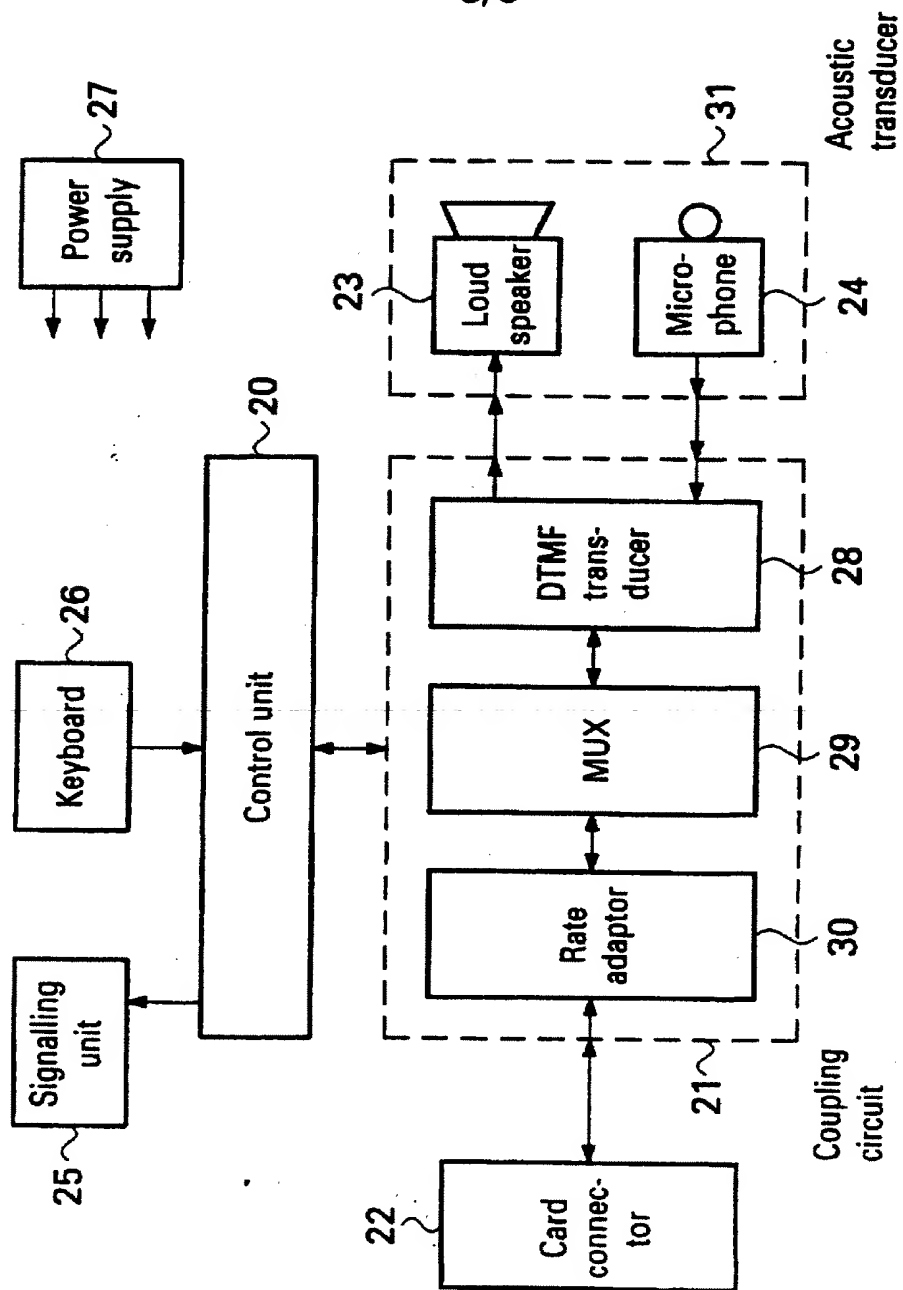


Fig. 4

4/6

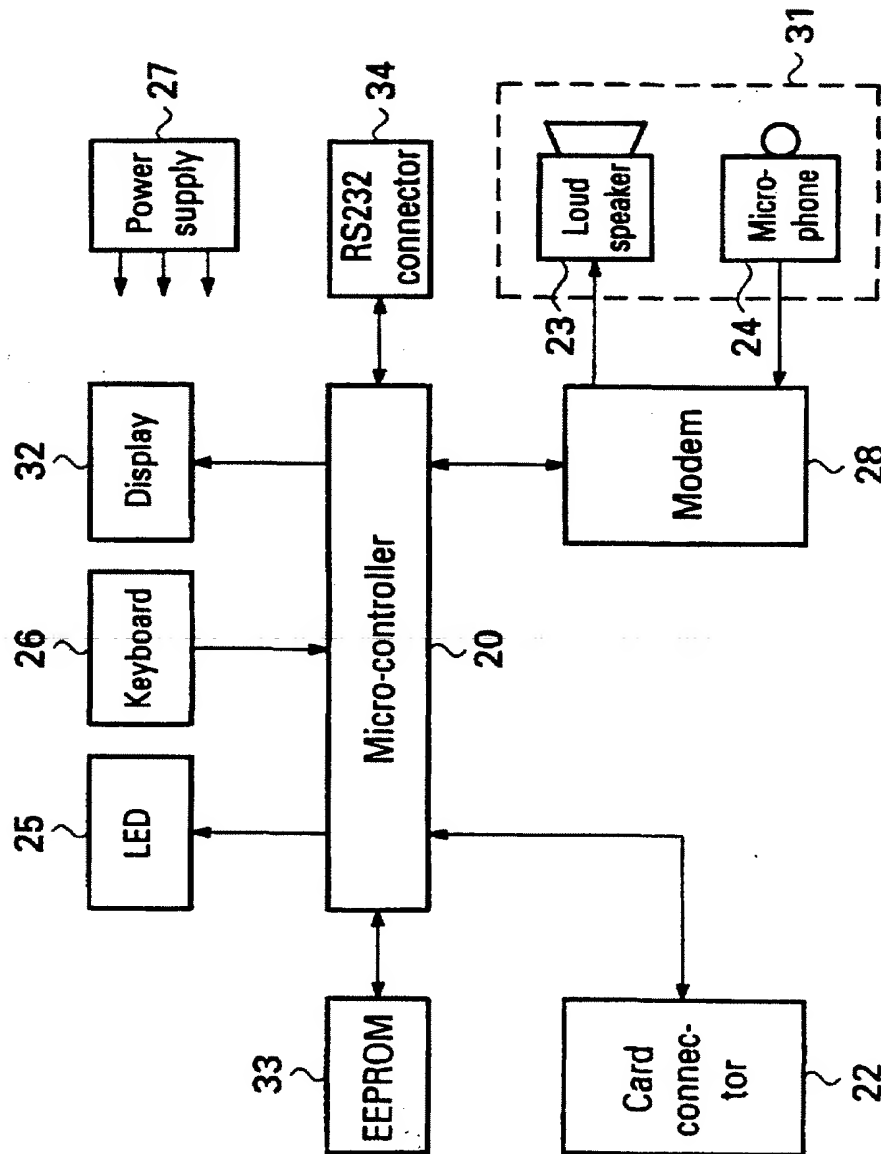


Fig. 5

5/6

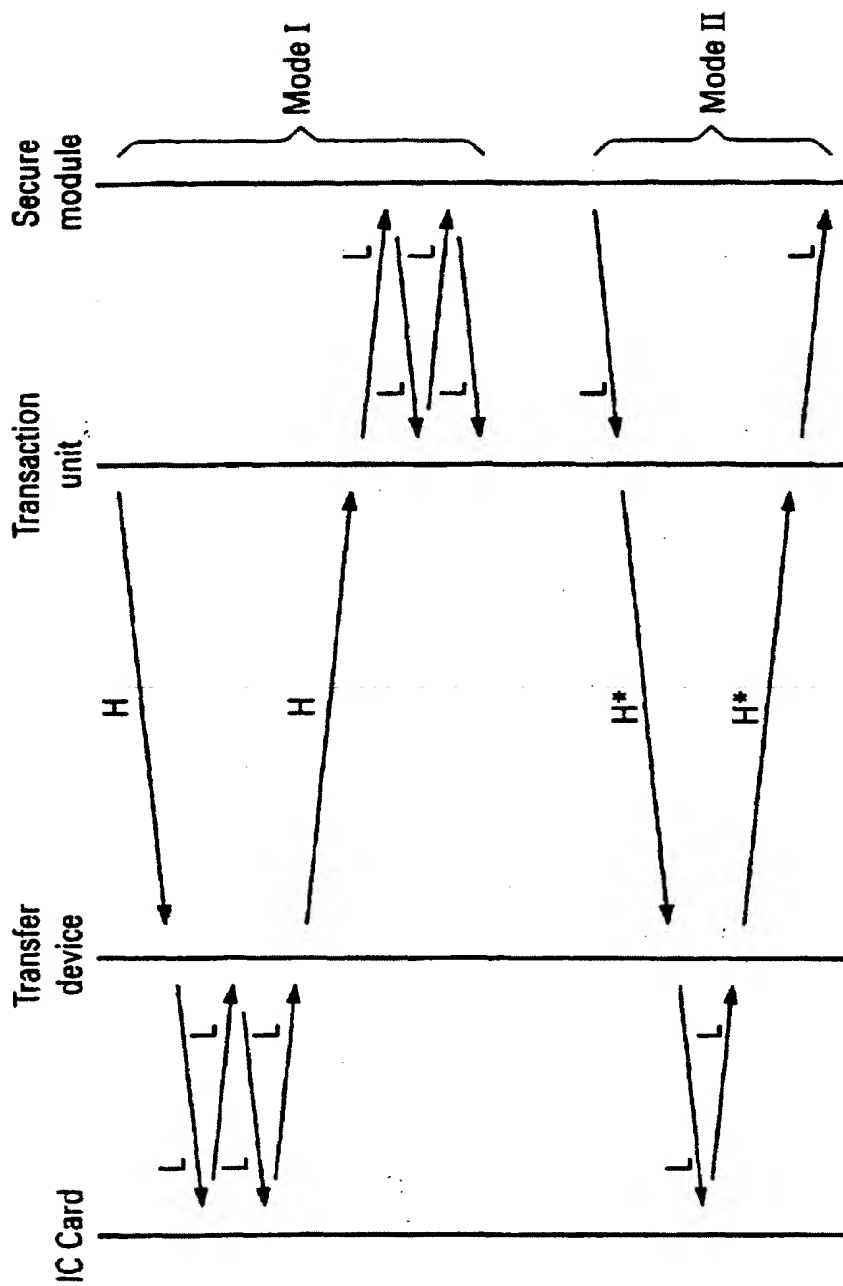
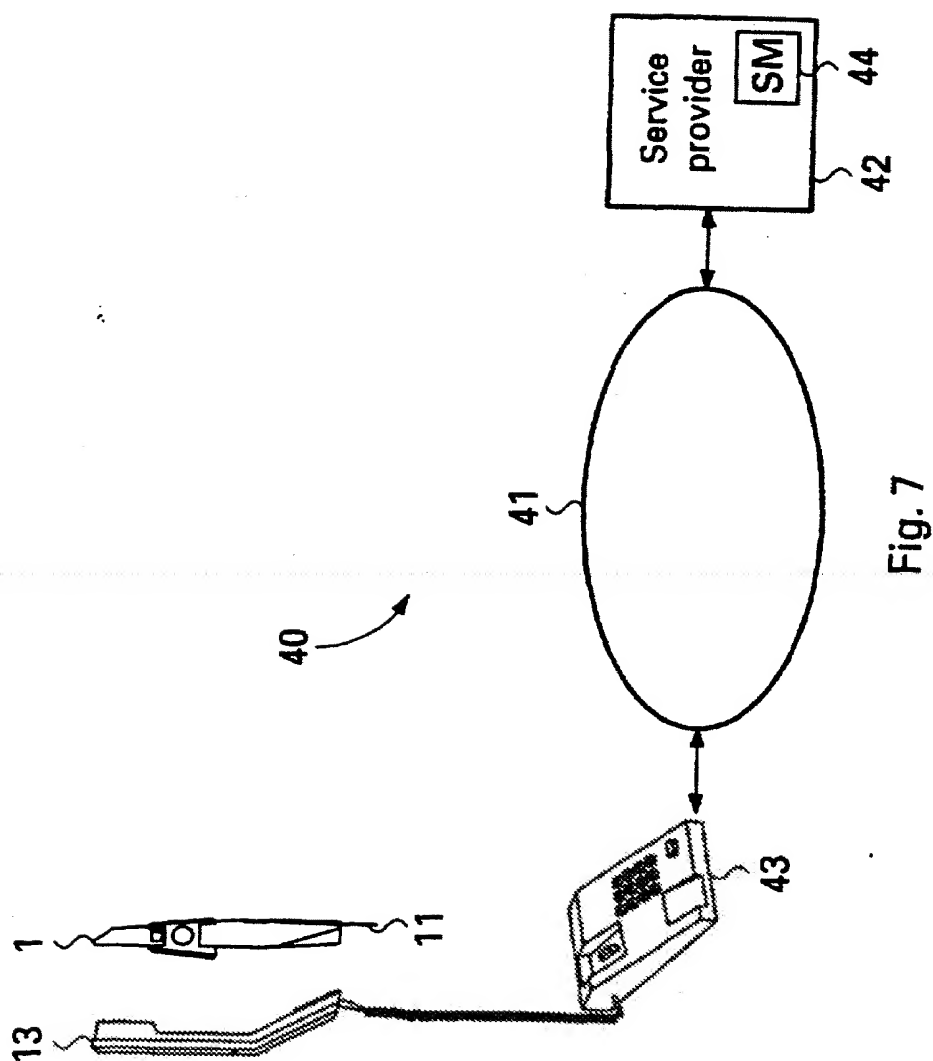


Fig. 6

6/6



INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP 96/01739

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04M1/00 G06K19/07 G06F15/02 G07B15/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04M G06K G06F G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US,A,5 189 287 (PARIENTI RAOUL) 23 February 1993 cited in the application see column 2, line 3 - column 5, line 50; figures 1-8	1,5,6, 8-10
Y	WO,A,95 04328 (INTELLECT AUSTRALIA PTY LTD) 9 February 1995 cited in the application see page 9, line 20 - page 16, line 19; figures 1-3 see page 35, line 25 - page 41, line 28 see page 64, line 11 - page 66, line 12	1,5,6, 8-10
A	---	2-4

	-/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is considered with one or more other such documents, such combinations being obvious to a person skilled in the art.

A document member of the same patent family

Date of the actual completion of the international search

30 August 1996

Date of making of the international search report

20.09.96

Name and mailing address of the ISA

European Patent Office, P.O. 5018 Patentkanal 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 540-2040, Tx. 31 631 epo nl,
Fax (+31-70) 540-3016

Authorized officer

Delangue, P

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/EP 96/01739

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO,A,91 07042 (NATIONAL TRANSACTION NETWORK INC) 16 May 1991 cited in the application see page 2, line 23 - line 36 see page 7, line 13 - page 17, line 17; figures 1-28 ---	1,6,8-10
A	GB,A,2 211 050 (GENERAL ELECTRIC CO PLC) 21 June 1989 see page 4, line 12 - page 8, line 26; figure 1 ---	1,5-7,10
A	WO,A,88 03294 (CALL IT CO) 5 May 1988 see page 6, line 3 - page 12, line 7; figures 1,2 ---	1,8-10
A	PATENT ABSTRACTS OF JAPAN vol. 011, no. 227 (E-526), 23 July 1987 & JP,A,62 043943 (CASIO COMPUT CO LTD), 25 February 1987, see abstract -----	1,6,8-10

INTERNATIONAL SEARCH REPORT

Continuation of patent family members

International Application No

PCT/EP 96/81739

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5189287	23-02-93	FR-A- 2648932 AT-T- 113138 AU-B- 5933898 CA-A- 2035462 DE-D- 69013470 DE-T- 69013470 EP-A- 0431138 ES-T- 2064740 WO-A- 9100574	28-12-90 15-11-94 17-01-91 24-12-90 24-11-94 11-05-95 12-06-91 01-02-95 10-01-91
WO-A-9504328	09-02-95	AU-B- 7341894 CA-A- 2168434 EP-A- 0711441	28-02-95 02-09-95 15-05-96
WO-A-9107042	16-05-91	US-A- 5050207 AU-B- 5187590 US-A- 5157717	17-09-91 31-05-91 20-10-92
GB-A-2211050	21-06-89	NONE	
WO-A-8803294	05-05-88	EP-A- 0289590 JP-T- 1502231	09-11-88 03-08-89